Perfect tight quantum teleportation without a shared reference

Verdon, Dominic ; Vicary, Jamie

DOI:
10.1103/PhysRevA.98.012306

Document Version
Publisher's PDF, also known as Version of record

Citation for published version (Harvard):
Verdon, D & Vicary, J 2018, 'Perfect tight quantum teleportation without a shared reference', *Physical Review A - Atomic, Molecular, and Optical Physics*, vol. 98, no. 1, 012306. https://doi.org/10.1103/PhysRevA.98.012306

Tight quantum teleportation without a shared reference frame

Dominic Verdon[*] and Jamie Vicary[†]
Department of Computer Science, Wolfson Building, University of Oxford, Parks Road, Oxford OX1 3QD, United Kingdom

(Received 3 October 2017; revised manuscript received 23 May 2018; published 9 July 2018)

We present a scheme for teleporting a quantum state between two parties whose local reference frames are misaligned by the action of a finite symmetry group. Unlike other proposals, our scheme requires the same amount of classical communication and entangled resources as conventional teleportation, does not reveal any reference frame information, and is robust against changes in reference frame alignment while the protocol is under way. The mathematical foundation of our scheme is a unitary error basis which is permuted up to a phase by the conjugation action of the group. We completely classify such unitary error bases for qubits, exhibit constructions in higher dimension, and provide a method for proving nonexistence in some cases.

DOI: 10.1103/PhysRevA.98.012306

I. INTRODUCTION

A. Motivation

It is now well recognized that a shared reference frame is an implicit assumption underlying the correct execution of many quantum protocols [1–6]. As quantum communication finds its way into handheld devices [7–9] and into space [10–12], it is increasingly important to develop protocols robust against reference frame error for situations where alignment is difficult [13–15] or undesired [16,17]. Considerable progress has already been made in this regard for quantum key distribution [18–24], and there is also a smaller body of work on quantum teleportation [25–27] without a shared reference frame, which our results extend.

B. Main results

We consider the problem of quantum teleportation between two parties whose local reference frames are misaligned, where the set of possible local reference frame transformations forms a finite group G with a unitary representation $\rho : G \to \mathrm{U}(d)$ on the d-dimensional system to be teleported. (This is the first paper in a series; the second paper [28] extends these results to the more common setting of infinite groups.) Success of the protocol is judged by a third-party observer who holds full reference frame information and who must agree that the original state has been teleported perfectly up to a global phase.[1] We present a teleportation scheme for certain (G,ρ), where G is finite, which is guaranteed to succeed regardless of the parties' reference frame configurations and which additionally satisfies the following properties.

(1) *Tightness*. The parties only require a d-dimensional maximally entangled resource state, and only 2 dits of classical information are communicated from Alice to Bob.

(2) *Dynamical robustness* (DR). The scheme is not affected by changes in reference frame alignment during transmission of the classical message from Alice to Bob.

(3) *No reference frame leakage* (NL). No information about either party's reference frame alignment is transmitted.[2]

Our scheme depends on the existence of a *G-equivariant unitary error basis* for the representation (G,ρ). We exhaustively classify these mathematical structures for two-dimensional representations, showing that they exist precisely when the image of the composite homomorphism $G \xrightarrow{\rho} \mathrm{U}(2) \xrightarrow{q} \mathrm{SO}(3)$ is isomorphic to 1, $\mathbb{Z}_2$, $\mathbb{Z}_3$, $\mathbb{Z}_4$, D_2, D_3, D_4, A_4, or S_4, where q is the quotient taking a unitary to its corresponding Bloch sphere rotation. We also provide a construction for any permutation representation with dimension less than 5 and show how to prove nonexistence in some cases.

Our results rely on an idea regarding the classical communication part of the protocol: We suppose that the readings of the classical channel are *themselves* interpreted with respect to the local reference frame. Mathematically, this corresponds to a nontrivial action of the group of reference frame transformations on the classical channel. Such classical channels have been called "unspeakable" [29]; we provide examples and show how they can be used to communicate the measurement result. An unspeakable classical channel is a powerful resource which could be used to execute a prior alignment step before the protocol begins, but we emphasize that it is *not* being used in this way here; indeed, by the (NL) property, our protocol in fact transfers no information at all about either party's reference frame alignment and makes use of the unspeakable channel in a nontrivial way.

We can give the following simple intuition for how our scheme works. Local reference frame misalignment can cause errors in the performance of the protocol, since Bob will perform correction operations with respect to his own frame, which need not be aligned with the frame in which Alice performed her measurement. But, since in our setting the

[*]dominic.verdon@cs.ox.ac.uk
[†]jamie.vicary@cs.ox.ac.uk

[1]This was called *unspeakable quantum teleportation* by Chiribella *et al.* [25].

[2]This has cryptographic significance in some scenarios [2,16,17].

misalignment also affects the classical channel, it can also cause errors in transmission of the classical measurement result; Bob may, in interpreting the channel reading with respect to his own frame, receive a different measurement value to that transmitted by Alice. In essence, our scheme is constructed so that these errors exactly cancel out. This intuition makes clear how the (DR) property is possible, since a change in local reference frame alignment also affects reception of the classical communication data, even if it takes place while that information is in transit.

C. Related work

Chiribella *et al.* [25] considered teleportation with a speakable classical channel only and showed that when the group G of reference frame transformations is a continuous compact Lie group, perfect tight teleportation is impossible; this does not contradict our work, which uses an unspeakable classical channel and a finite group G. (Furthermore, as a consequence of our main results, we show that for finite G, perfect tight teleportation is indeed possible with a speakable classical channel in some restricted situations; see Corollary II.9 and Remark IV.2.)

Several other solutions for reference frame–independent teleportation for a finite group of reference frame transformations exist in the literature. These all involve establishment of a shared reference frame in some way: by using preshared entanglement [25], sharing entanglement during the protocol [2], or transmitting more complex resources [1, Sec. V A]. Unlike our scheme, these approaches work for arbitrary (G,ρ), where G is finite. However, none of them have all the properties of tightness, dynamical robustness, and no reference frame leakage, as our scheme does.

Quantum communication under collective noise corresponding to a finite group was considered by Skotiniotis *et al.* [30]. From the perspective of our discussion above, their protocol satisfies the (DR) and (NL) properties. However, it requires a quantum channel; it is not a teleportation protocol. Their token could be equally be transmitted using an unspeakable classical channel of the type we construct in Sec. III. However, we are not transmitting a token in their sense; in particular, the classical system we transmit need not carry a free and transitive action of G.

D. Criticism

We can criticize our scheme as follows. First, as with the alternative solutions discussed above, it works only for finite G (although we discuss a related scheme for the case of infinite G in a successor article [28]). Second, it cannot be implemented for all scenarios (G,ρ) with finite G, and, although we provide a range of constructions of equivariant unitary error bases and completely characterize valid (G,ρ) for qubit teleportation, we cannot give necessary and sufficient conditions for the applicability of our scheme in higher dimensions. Third, to communicate the measurement result, we do not use an ordinary "speakable" classical channel, but rather an "unspeakable" classical channel; while we provide a number of examples of such channels, it is nevertheless clear that this aspect of our approach may raise technological barriers in an implementation. Finally, up to a global phase, the system to be teleported and Bob's half of the entangled pair must carry the same representation ρ of G, and Alice's half of the entangled pair must transform according to the dual representation ρ^*; although this is physically reasonable in view of charge conservation, a situation may arise in which it is hard to construct a system carrying the representation ρ^*. Very often (for instance, for all representations with real characters), $\rho \simeq \rho^*$ up to a phase, which solves this problem.

E. Outlook

These results may be applicable to cryptography and security of quantum protocols, as it has been noted that reference frame uncertainty is of cryptographic importance [2,16,17] and that a private shared reference frame may be considered as a secret key [16,17]. In this context, it is useful to know what protocols, such as quantum teleportation, may be performed even in the absence of a shared reference frame, without any transmission of cryptographically sensitive reference frame information.

We can also build on these results to produce schemes for teleportation with a continuous compact Lie group of reference frame transformations. This is treated in a forthcoming paper [28].

F. Outline

In Sec. II, we present our scheme for reference frame–independent teleportation, beginning with an informal example for a group of spatial reference frame transformations. Our scheme uses an unspeakable classical channel carrying a certain action; in Sec. III, we show how these may be constructed and give several examples. Finally, in Sec. IV, we turn our attention to the problem of classifying and constructing equivariant unitary error bases, on which our scheme depends.

II. REFERENCE FRAME–INDEPENDENT TELEPORTATION

A. Example

1. Scenario

Alice and Bob are quantum information theorists operating on spin-$\frac{1}{2}$ particles. They work in separate laboratories, which do not necessarily have the same orientation in space, and their task is to teleport a quantum state without revealing their spatial orientations, either to each other or to any eavesdropper. Their relative orientations are not completely unknown: The rotation g taking Alice's Cartesian frame onto Bob's is promised to lie within the subgroup $\mathbb{Z}_3 \subset \mathrm{SO}(3)$, the group of rigid spatial rotations through multiples of $2\pi/3$ radians around some axis. However, $g \in \mathbb{Z}_3$ is unknown. Let $a \in \mathbb{Z}_3$ be the transformation rotating the reference frame anticlockwise through $2\pi/3$ radians. We suppose that the action of a affects the description of qubit states by the standard spin-$\frac{1}{2}$ representation:

$$\rho(a) = \begin{pmatrix} 1 & 0 \\ 0 & e^{2\pi i/3} \end{pmatrix}. \tag{1}$$

That is, a state which appears as $|v\rangle$ in frame configuration f will appear as $\rho(a)\,|v\rangle$ in frame configuration af.

Alice and Bob share the two-qubit entangled state

$$|\eta\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle).$$

Note that this state is invariant up to a phase under the action (1) of a change in reference frame orientation, so the entanglement will not be degraded by changes in reference frame alignment following its initialization. All these aspects of the overall setup are common knowledge to both parties.

2. The conventional protocol

A conventional quantum teleportation scheme [31] is presented in terms of a *unitary error basis* (a family of unitary operators which form an orthogonal basis for the operator space under the trace inner product):

$$U_0 = \begin{pmatrix} 1 & 0 \\ 0 & e^{2\pi i/3} \end{pmatrix}, \quad U_2 = \frac{1}{\sqrt{3}}\begin{pmatrix} 1 & \sqrt{2}e^{2\pi i/3} \\ \sqrt{2} & e^{5\pi i/3} \end{pmatrix},$$
$$U_1 = \frac{1}{\sqrt{3}}\begin{pmatrix} 1 & \sqrt{2}e^{4\pi i/3} \\ \sqrt{2}e^{4\pi i/3} & e^{5\pi i/3} \end{pmatrix}, \tag{2}$$
$$U_3 = \frac{1}{\sqrt{3}}\begin{pmatrix} 1 & \sqrt{2} \\ \sqrt{2}e^{2\pi i/3} & e^{5\pi i/3} \end{pmatrix}.$$

The scheme proceeds as follows. Alice measures her initial system together with her half of the entangled state in a maximally entangled orthonormal basis $|\phi_i\rangle = (\mathbb{1} \otimes (U_i X)^T)\,|\eta\rangle$, where X is the Pauli X matrix,[3] and communicates the result i to Bob through an ordinary classical channel, which transmits the measurement result faithfully. Bob then applies the correction U_i to his half of the entangled state.

If the reference frames have the same alignment, the procedure will be successful. However, if the reference frames are misaligned by some nonidentity element $g \in \mathbb{Z}_3$, then, from the perspective of Alice's frame, Bob will not perform the intended correction U_i, but rather $\rho(g)^\dagger U_i \rho(g)$. Assuming the uniform distribution over $\mathbb{Z}_3$, a simple calculation shows that an input pure state will emerge in a mixed state.

3. Our protocol

We now describe our reference frame–independent scheme. Before performing the protocol, Alice and Bob share the coordinates of four unit vectors $\{\boldsymbol{v}_0, \boldsymbol{v}_1, \boldsymbol{v}_2, \boldsymbol{v}_3\} \in \mathbb{R}^3$, which form a regular tetrahedron centered on the origin such that, under the reference frame transformation $a \in \mathbb{Z}_3 \subset \mathrm{SO}(3)$, the vectors are permuted as follows:

$$a \cdot \boldsymbol{v}_0 = \boldsymbol{v}_0 \quad a \cdot \boldsymbol{v}_1 = \boldsymbol{v}_2 \quad a \cdot \boldsymbol{v}_2 = \boldsymbol{v}_3 \quad a \cdot \boldsymbol{v}_3 = \boldsymbol{v}_1. \tag{3}$$

For example, let $\boldsymbol{v}_0 = \frac{1}{\sqrt{3}}(\hat{\boldsymbol{x}} + \hat{\boldsymbol{y}} + \hat{\boldsymbol{z}})$, $\boldsymbol{v}_1 = \frac{1}{\sqrt{3}}(\hat{\boldsymbol{x}} - \hat{\boldsymbol{y}} - \hat{\boldsymbol{z}})$, $\boldsymbol{v}_2 = \frac{1}{\sqrt{3}}(-\hat{\boldsymbol{x}} + \hat{\boldsymbol{y}} - \hat{\boldsymbol{z}})$ and $\boldsymbol{v}_3 = \frac{1}{\sqrt{3}}(-\hat{\boldsymbol{x}} - \hat{\boldsymbol{y}} + \hat{\boldsymbol{z}})$, and suppose that the generating element $a \in \mathbb{Z}_3$ acts as a right-handed rotation about the axis defined by $\boldsymbol{v}_0$.

If Alice obtains measurement result i, she communicates this to Bob in the following way: She prepares a physical arrow, of the sort a medieval archer might use, arranges it to have the same orientation as the vector $\boldsymbol{v}_i$, and then sends it directly to Bob by parallel transport along a known path. When the arrow is received, Bob observes its orientation in his own frame, correcting if necessary for the parallel transport map associated to the path, and matches this with one of the reference orientations $\boldsymbol{v}_j \in \{\boldsymbol{v}_0, \boldsymbol{v}_1, \boldsymbol{v}_2, \boldsymbol{v}_3\}$; he thus obtains the message $j \in \{0,1,2,3\}$. He then performs the corresponding unitary correction. This procedure is illustrated in Fig. 1.

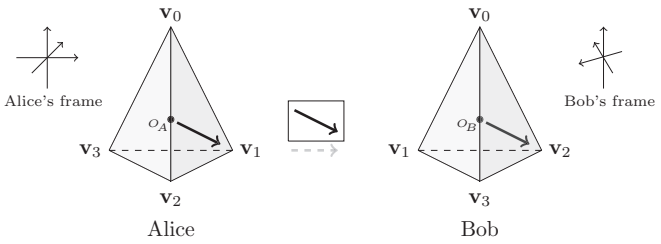


FIG. 1. In our classical communication procedure, Alice and Bob label the vertices of regular tetrahedra centered on their origins O_A and O_B, using their own Cartesian frames. Bob's frame is related to Alice's by a $2\pi/3$ anticlockwise rotation around the axis defined by $\boldsymbol{v}_0$. Upon measuring $|\phi_1\rangle$, Alice prepares an arrow pointing to vertex $\boldsymbol{v}_1$ and sends this to Bob by parallel transport. In Bob's frame, this arrow points to vertex $\boldsymbol{v}_2$, and so he performs correction U_2.

Note that Alice transmits no information about her local reference frame by the above procedure, since her measurement result is uniformly random, and thus so is the direction indicated by the arrow. Also, we emphasize that exactly two bits of classical information have been transferred, since there were four possible values upon transmission and four possible values upon receipt.

Suppose that Alice and Bob's laboratories share the same reference frame; that is, their local frames are related by the element $e \in \mathbb{Z}_3$ of the group of reference frame transformations. Then the arrow's orientation will be the same in Bob's frame as in Alice's frame, and the measurement outcome will be faithfully communicated. In this case, the protocol will be successful, and it is identical to the conventional teleportation protocol, albeit with the two classical bits of information transmitted from Alice to Bob in an unusual way.

Now suppose that Alice and Bob's frames are misaligned by the action of the element $a \in \mathbb{Z}_3$ of the reference frame transformation group. In this case, if Alice sends the result 0, 1, 2, or 3, Bob will receive the result 0, 2, 3, or 1 respectively, because of the transformation properties (3) of the arrows. Furthermore, when Bob applies the unitary U_i in his local frame, its action is seen in Alice's frame as $\rho(a)^\dagger U_i \rho(a)$. The following equations describe the consequences of such a conjugation, as can be directly checked using expressions (1) and (2):

$$\rho(a)^\dagger U_0 \rho(a) = U_0, \qquad \rho(a)^\dagger U_1 \rho(a) = U_3,$$
$$\rho(a)^\dagger U_2 \rho(a) = U_1, \qquad \rho(a)^\dagger U_3 \rho(a) = U_2.$$

We now see the point of the entire construction: The unitary error basis (2) was carefully chosen so that these two apparent sources of error—in the transmission of the classical measurement result and in Bob's unitary correction—exactly cancel

[3]The Pauli X matrix appears because of the choice of entangled state η.

each other out. For example, if Alice obtains measurement outcome 1, Bob will receive this as measurement outcome 2, and will perform the correction U_2 in his frame, which in Alice's frame is equal to $\rho(a)^\dagger U_2 \rho(a) = U_1$, and so the intended correction will be carried out after all. As a result, the quantum teleportation will conclude successfully, even though Alice and Bob's reference frames were misaligned. Similarly, it can be shown that the teleportation is also successful if the frame misalignment is given by the element $a^2 \in \mathbb{Z}_3$.

4. Discussion

We have exhibited a procedure for reference frame–independent quantum teleportation in the particular case of spatial reference frame misalignment with transformation group $\mathbb{Z}_3 \subset \mathrm{SO}(3)$. This involved a careful choice of unitary error basis (2), with communication of the measurement result through a classical channel carrying a compatible nontrivial action (3) of the reference frame transformation group. Only two bits of classical information were transferred from Alice to Bob, as in a conventional teleportation procedure, and the Hilbert space of the entangled resource was of minimal dimension, so this procedure was *tight* in the sense of Werner [31]. The unspeakable information transmitted by Alice was uniformly random, since Alice's measurement results were; in particular, Bob, or an eavesdropper on the classical channel, received no information about Alice's reference frame alignment. Finally, the procedure would have succeeded even if Bob's reference frame alignment changed during the protocol, while Alice's measurement result was still in transit.

In this example, we chose $\mathbb{Z}_3 \subset \mathrm{SO}(3)$ as the reference frame transformation group, but the same unitary error basis and classical channel allow reference frame–independent teleportation for the group $A_4 \subset \mathrm{SO}(3)$ of order 12, as we will see in Sec. IV.

B. General scheme

We now present our scheme in full generality. We begin by recalling the conventional teleportation protocol.

Procedure II.1 (Conventional tight teleportation [32]). Alice holds an n-dimensional quantum system, prepared in a state $|\psi\rangle$. Separately, Alice and Bob hold an entangled pair of n-dimensional quantum systems, in a maximally entangled state $(1 \otimes X)\,|\eta\rangle$ for some unitary X, where

$$|\eta\rangle = \frac{1}{\sqrt{n}} \sum_{i=1}^{n} |ii\rangle$$

is the generalized Bell state.[4] Alice performs a joint measurement on the system to be teleported and her entangled system, described by an orthonormal basis $|\phi_i\rangle \in \mathbb{C}^n \otimes \mathbb{C}^n$. She communicates the classical measurement result i to Bob using a perfect classical channel; Bob then performs the unitary correction U_i on his half of the entangled state. The procedure is successful if Bob's system is now in the state $|\psi\rangle$.

[4]All maximally entangled states of a bipartite system are of this form.

A complete description of correct procedures was given by Werner, who showed that they can be characterized mathematically in terms of unitary error bases.

Definition II.2. For a Hilbert space H, a *unitary error basis* (UEB) is a basis of unitary operators $\{U_i\}_{i\in I}$, with $I = \{0,1,\ldots,\dim(H)^2 - 1\}$, such that for all $i,j \in I$ we have

$$\mathrm{Tr}(U_i^\dagger U_j) = \delta_{ij} \dim(H). \tag{4}$$

Under this correspondence, we construct Alice's joint measurement basis as

$$|\phi_i\rangle := \left(\mathbb{1} \otimes X^{\mathrm{T}} U_i^{\mathrm{T}}\right) |\eta\rangle, \tag{5}$$

and Bob performs the correction U_i from the unitary error basis when he receives the measurement result i from Alice. Werner showed [31, Theorem 1] that all correct measurement and correction data for Procedure II.1 can be obtained from a unitary error basis in this way.

A second key concept in our scheme is that of an *unspeakable classical channel*. For simplicity, we only consider perfect classical channels in this paper; whatever reading Alice sends through the channel will be received unaltered by Bob. However, his interpretation of this reading will be affected by his reference frame orientation.

Definition II.3. For a finite group G, an *unspeakable classical channel* is a classical channel whose set of messages carries a nontrivial action of the group G of reference frame transformations.

Writing I for the set of messages carried by the channel, we can encode the data of an unspeakable channel as a group action $\sigma : G \times I \to I$. For each reference frame transformation $g \in G$ taking Alice's frame onto Bob's frame, we obtain an invertible function $\sigma(g,-) : I \to I$, which describes how a message input by Alice using her local frame is interpreted by Bob with respect to his local frame. Since this function is invertible, there is no loss of information; however, if the receiver of the message does not know $g \in G$, they will be unable to infer which message was actually input. The arrows channel of Sec. II A was an unspeakable classical channel; we will see more examples in Sec. III.

We now define our teleportation scheme. Here we write ρ^* for the dual representation of ρ.

Procedure II.4 (Reference frame–independent teleportation). Alice has an n-dimensional quantum system in a state $|\psi\rangle$. Separately, Alice and Bob hold a maximally entangled state $(\mathbb{1} \otimes X)\,|\eta\rangle$ of a pair of n-dimensional quantum systems. They each possess local reference frames with transformation group G, acting unitarily by a representation ρ on the system to be teleported, by a representation $\rho^* \otimes \theta_1$ on Alice's half of the entangled state, and by a representation $\rho \otimes \theta_2$ on Bob's half of the entangled state, where θ_1,θ_2 are any one-dimensional representations of G.

Alice performs a joint measurement on the system to be teleported and her half of the entangled state, described by an orthonormal basis $\{|\phi_i\rangle\}$, $|\phi_i\rangle \in \mathbb{C}^n \otimes \mathbb{C}^n$. She uses a perfect unspeakable classical channel to communicate the classical measurement result i to Bob, who receives the message $\sigma(g,i)$, where g is the transformation taking Alice's local frame configuration upon transmission onto Bob's local frame

configuration upon receipt. Bob then immediately performs a unitary correction $U_{\sigma(g,i)}$ on his half of the entangled state.

Remark II.5. We prove in Appendix A that the conditions on the possible representations carried by each system precisely imply that the maximally entangled state may always be taken to be G invariant up to a phase, preventing degradation of entanglement by reference frame transformations.

The measurement and correction operations for Procedure II.4, together with the action σ on the unspeakable classical channel, are *correct data* if, regardless of Alice and Bob's reference frame alignments, Bob's system ends in the state $|\psi\rangle \in \mathbb{C}^n$, according to a third observer with a fixed frame who can see both laboratories.

Definition II.6 (G-equivariant unitary error basis). For a finite group G, and a Hilbert space H carrying a unitary action ρ of G, an *equivariant unitary error basis* for (G,ρ) is a unitary error basis $\{U_i\}_{i\in I}$ for H whose elements are permuted up to a phase[5] by the right conjugation action of G.

That is, for all $i \in I$ and $g \in G$, and some family of phases $\xi(i,g) \in \mathbb{C}$, we have that $\xi(i,g)\rho(g)^\dagger U_i \rho(g) \in \{U_i\}_{i\in I}$. Ignoring the phases, we can encode the effect of this conjugation as a right group action $\tau : I \times G \to I$.

We now show that the notion of G-equivariant unitary error basis gives a precise mathematical characterization of correct data for Procedure II.4.

Theorem II.7. All correct data for Procedure II.4 can be obtained from an equivariant unitary error basis $\{U_i\}$ for (G,ρ), with associated right action τ. The measurement and correction operations are as in (5), and the unspeakable classical channel carries the action $\tau^{-1} : G \times I \to I$.

Proof. We work in Alice's frame. Let Bob's misalignment with respect to this frame be $g \in G$. For sufficiency, suppose Alice measures $x \in I$; Bob then reads $\tau^{-1}(g,x)$ and performs the correction

$$U_{\tau(\tau^{-1}(g,x),g)} = U_x,$$

as required. For necessity, note that the procedure must work for trivial misalignment $g = e$; therefore, by Werner's result [31, Theorem 1], Alice must perform measurements corresponding to a unitary error basis, and Bob must perform the unitary correction U_x in his own frame whenever he receives $x \in I$. The condition on the unspeakable channel is therefore clear. ∎

We say that an unspeakable classical channel is *compatible* with an equivariant UEB when it carries the inverse action as in Theorem II.7. We see that our scheme can be implemented for some representation (G,ρ) if and only if there exists an equivariant UEB for (G,ρ), and Alice and Bob have access to a compatible unspeakable classical channel. Before investigating these requirements, we draw a straightforward corollary from Theorem II.7.

Definition II.8 (Orbit type). For a G-equivariant unitary error basis $\{U_i\}_{i\in I}$, we define its *orbit type* as the multiset of sizes of each orbit in I under the action $\tau : I \times G \to I$.

Corollary II.9. With only a speakable classical channel (that is, a channel carrying a trivial G action), Procedure II.4 succeeds for all frame alignments only if the action $\tau : I \times G \to I$ is trivial; that is, the elements of the orbit type of the equivariant UEB are all 1.

III. UNSPEAKABLE CHANNELS

In this section, we address the physical requirement of our scheme, a compatible unspeakable classical channel for a given equivariant UEB.

A. Construction from quantum systems

We begin with a completely general method for constructing such a channel. When Alice performs the measurement on her two systems, they decohere in her measurement basis, and the joint system becomes a single classical object. Alice can transfer this directly to Bob, still in the eigenstate corresponding to her measurement result. Since the reference frame transformation is guaranteed to act as a permutation on measurement outcomes, Bob will also receive the system in an eigenstate, which he can can identify by performing the same measurement as Alice. Because of reference frame uncertainty, the result he receives may of course be different than that noted by Alice. The result is an unspeakable classical channel. Since Bob both measures and performs the corresponding corrections in his own frame, the procedure will succeed for any reference frame misalignment.

B. Construction from shared classical system

In some physical situations, the method of Sec. III A involving transfer of the decohered quantum systems may be impractical. We now provide an alternative construction. The problem is the following: Given the right action $\tau : I \times G \to I$ of a finite group on a finite index set, we must construct a compatible unspeakable classical channel Σ whose set of messages M_Σ can be identified with I, so that it carries the corresponding left action $\tau^{-1} : G \times I \to I$.

Here we show how this can be done when τ^{-1} is a transitive action. This is sufficient since, if τ^{-1} is not transitive, I will split into orbits under it, and the following procedure may be performed:

(1) After her measurement, Alice communicates the orbit $O \subset I$ of the index she measured, through a speakable channel.

(2) She then communicates the precise measurement index $i \in O$ using an unspeakable classical channel with the set of messages O, carrying the restricted action $\tau^{-1}|_O : G \times O \to O$, which is transitive.

This procedure still leaks no reference frame information, since the orbit is communicated as speakable information and the outcomes within each orbit are equiprobable. It is still tight, since the classical channel distinguishes only d^2 possible messages, despite being split into speakable and unspeakable parts. It is still dynamically robust, since the orbit is unaffected by reference frame transformations.

We assume, therefore, that the action τ^{-1} is transitive. We can then characterize it further using the following well-known fact from group theory. Recall that the set of right cosets $\{Hg_i\}$

[5] In an early version of this work [33], we used the term *G equivariant* for the specific situation where $\xi(i,g) = 1$. Here we choose to make this more general definition, since it is more physically relevant.

of a subgroup $H < G$ carries a canonical left action $g(Hg_i) = Hg_ig^{-1}$; we write this left G set as G/H.

Lemma III.1. For any transitive left G set X, there is a unique conjugacy class C of subgroups of G such that $X \simeq G/H$ if and only if (iff) $H \in C$.

It follows that τ^{-1} is characterized up to isomorphism by its associated conjugacy class of subgroups. It also follows that any *transitive* unspeakable classical channel Σ (that is, any unspeakable classical channel whose set of messages M_Σ is a transitive G set) is characterized by its associated conjugacy class of subgroups C_Σ. Our problem can therefore be rephrased as follows: We need to construct a transitive unspeakable channel for which $C_\Sigma = C_{\tau^{-1}}$, so that $M_\Sigma \simeq G/H \simeq I$ as left G sets.

A key construction is the following, which allows us to group together messages in M_Σ to create a new channel with a different associated conjugacy class.

Construction III.2 (Quotient channel). Let Σ be a transitive unspeakable classical channel with associated conjugacy class of subgroups C_Σ, and let $H_\Sigma \in C_\Sigma$. Fix an isomorphism $\alpha : M_\Sigma \simeq G/H_\Sigma$. Let K be another subgroup such that $H_\Sigma < K < G$.

We obtain a *quotient channel* whose associated conjugacy class of subgroups has representative K, and whose messages are right cosets Kg, transmitted as follows. In order to send a coset Kg, Alice picks uniformly at random any element $x \in K/H_\Sigma \subset G/H_\Sigma$ and sends the message $\alpha^{-1}(xg) \in M_\Sigma$. Depending on his reference frame orientation, Bob receives some $y \in M_\Sigma$, such that $\alpha(y)$ lies in some right coset of K/H_Σ. He then uses the canonical isomorphism

$$\frac{G/H_\Sigma}{K/H_\Sigma} \simeq G/K$$

to obtain a right coset of K in G, which is the message he receives.

We obtain the following corollary. Recall the usual partial order on conjugacy classes of subgroups, where $C_1 < C_2$ iff $H_1 < H_2$ for some $H_1 \in C_1, H_2 \in C_2$.

Corollary III.3. If we have access to a transitive unspeakable classical channel Σ with associated conjugacy class of subgroups C_Σ, and $C_\Sigma < C_{\tau^{-1}}$, then we may construct a compatible channel for τ.

Proof. Take $H_{\tau^{-1}} \in C_{\tau^{-1}}$, $H_\Sigma \in C_\Sigma$ such that $H_\Sigma < H_{\tau^{-1}}$, and construct the quotient channel. ■

The trivial subgroup is the only member of its conjugacy class, which we call the *trivial class*. The trivial class is the minimal element of the poset of conjugacy classes of subgroups. It follows that from an transitive unspeakable channel Σ whose associated conjugacy class of subgroups is the trivial class, we may construct a compatible channel for any transitive τ^{-1}.

We now show how to use a shared classical system to construct an unspeakable classical channel with trivial associated conjugacy class.

Definition III.4. A *reference frame system* is a classical system whose configuration is described according to a local reference frame and whose set of configurations C carries a free and transitive action of G.

The details of how this system is shared between Alice and Bob are abstracted away in this approach. The nomenclature is derived from the fact that Alice and Bob each possess physical systems serving as their local reference frames, on which the reference frame transformation group G acts freely and transitively, by definition.

Alice and Bob will use their shared reference frame system to communicate messages. They associate each of the $|G|$ configurations of the system to an element of G using a *labeling*, which is a choice of isomorphism $l : C \to G$ depending on their local reference frame configurations. Once Alice fixes a labeling, she can communicate element $g \in G$ to Bob by preparing the system in the configuration associated to g in her labeling. Bob will then interpret this configuration with respect to his own labeling.

A labeling $l : C \to G$ is obtained by choosing a configuration x_e such that $l(x_e) = e$; the labeling is then fully determined by the equation $l(gx_e) = gl(x_e) = g$. Alice and Bob both agree on a way to pick x_e based on their own local frame configuration; this is specified by a map $\epsilon : \mathcal{F} \to C$, where $\mathcal{F}$ is the space of local frame configurations and ϵ satisfies the naturality equation

$$\epsilon(gf) = g\epsilon(f).$$

We write $[l(x)]$ to refer to $x \in C$ when a labeling is fixed. Alice and Bob generally have different labelings l_A, l_B, so we write $[l_A(x)]_A$, $[l_B(x)]_B$ to refer to x using their respective labelings. We obtain the following proposition.

Proposition III.5. A shared reference frame system gives rise to a transitive unspeakable classical channel whose associated conjugacy class of subgroups is trivial.

Proof. From the above discussion, the labeling of the channel is defined as $[g]_A = g[e]_A$; we have $[e]_A = \epsilon(f_A)$, so $[g]_A = g\epsilon(f_A) = g\epsilon(g_{AB}^{-1} f_B) = (gg_{AB}^{-1}) \cdot [e]_B = [gg_{AB}^{-1}]_B$. The channel therefore carries the action $\sigma(g,x) = xg^{-1}$, and the result follows. ■

By Corollary III.3, it is therefore possible to construct a compatible unspeakable channel for any equivariant unitary error basis using a shared reference frame system. We conclude this section by presenting two examples of shared reference frame systems.

Example III.6 (Particle in a box). Suppose that the quantum systems used in the teleportation protocol are particles in cubic boxes. In order to describe states of and operations on these systems, it is necessary to decide which sides of the box are "up," "front," and "right." Alice and Bob shared such a labeling when they created their entangled pair of boxes; since that time, however, the orientation, and therefore the labeling, of Bob's box may have altered. The choice of labeling can be seen as a reference frame, whose transformation group is the group of rigid rotations of a cube. One reference frame system here is a classical solid cube, with labeled sides, passed between parties; the map $\epsilon : \mathcal{F} \to C$ is defined by labeling the cube identically to the box containing the particle. This is illustrated in Fig. 2.

Example III.7 (Group of time translations). We suppose that the system to be teleported has a basis of energy eigenstates with different energy eigenvalues. Over the period T of time evolution, these states will acquire a relative phase. In order to define states and operations, Alice and Bob must choose a time t_0 at which the chosen basis vectors will have trivial phase. If we are promised that Alice and Bob's clocks are related by a

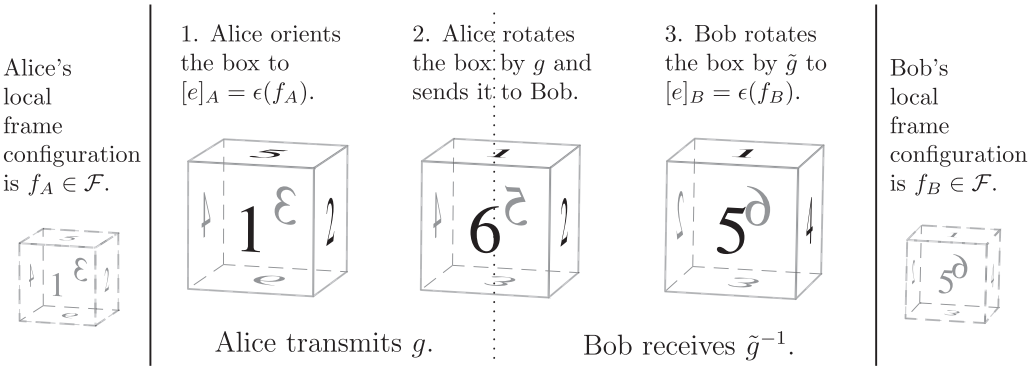


FIG. 2. The reference frame channel of Example III.6, where G is the group of rigid rotations of a cube. Here Alice transmits a $\pi/2$ rotation around the x axis, and Bob receives a π rotation around the z axis.

time translation in a finite subgroup of U(1), then the choice of t_0 corresponds to a reference frame with cyclic transformation group. One reference frame system here is the time of arrival, modulo T, of a signal transmitted from Alice to Bob; the map $\epsilon : \mathcal{F} \to C$ is defined by the signal arriving at one's own time t_0.

IV. EQUIVARIANT UNITARY ERROR BASES

We now turn to the classification and construction of equivariant unitary error bases, the mathematical basis for our scheme.

A. Classification for qubits

We first fully classify equivariant UEBs for two-dimensional representations (G,ρ). Let $q : \mathrm{SU}(2) \to \mathrm{SO}(3)$ be the quotient homomorphism taking a qubit unitary to its corresponding Bloch sphere rotation. Our results are outlined in the following theorem.

Theorem IV.1 (Classification of equivariant UEBs for qubits). The existence of unitary error bases of a given orbit type for a unitary representation $\rho : G \to \mathrm{U}(2)$ depends only on the isomorphism class of the image subgroup $q(\rho(G)) \subset \mathrm{SO}(3)$, according to the classification given in Table I .

The proof of the classification is given in Appendix B. While in Table I, we have only given the orbit type of the UEBs, in Appendix B we also describe the associated action $\tau : I \times G \to G$.

Remark IV.2. By Corollary II.9, tight qubit teleportation without an unspeakable classical channel is possible only when the image of the composite homomorphism $G \xrightarrow{\rho} \mathrm{U}(2) \xrightarrow{q} \mathrm{SO}(3)$ is isomorphic to 1, $\mathbb{Z}_2$ or D_2.

B. Higher dimensions

In this section, we consider the problem of constructing an equivariant UEB for representations of dimension greater than two.

TABLE I. UEB families for qubit representations.

Isom. class of $q(\rho(G))$	Orbit types and solutions, up to phase	Further details
Trivial	(1,1,1,1), any UEB	N/A
$\mathbb{Z}_2$	(1,1,1,1), one 2-parameter family	Proposition B.8
	(2,1,1), one 2-parameter family	
	(2,2), one 2-parameter family	
$\mathbb{Z}_3$	(3,1), one 2-parameter family	Proposition B.9
$\mathbb{Z}_4$	(2,1,1), one 2-parameter family	Proposition B.10
$\mathbb{Z}_n, n \geqslant 5$	No solutions	N/A
D_2	(1,1,1,1), one isolated solution	Proposition B.12
	(2,1,1), six isolated solutions	
	(2,2), three isolated solutions	
	(4), two isolated solutions	
D_3	(3,1), six isolated solutions	Proposition B.13
D_4	(2,1,1), two isolated solutions	Proposition B.14
	(2,2), two isolated solutions	
$D_n, n \geqslant 5$	No solutions	N/A
Tetrahedral (A_4)	(4), two isolated solutions	Proposition B.16
Octahedral (S_4)	(1,3), one isolated solution	Proposition B.17
Icosahedral (A_5)	No solutions	N/A

1. Constructions for permutation representations

Recall that a representation $\rho : G \to U(n)$ is a *permutation representation* if there exists an orthonormal basis of $\mathbb{C}^n$ in which $\rho(g)$, $g \in G$ are all permutation matrices. In this special case, equivariant UEBs can be constructed from Hadamard matrices satisfying a certain equivariance condition.

Proposition IV.3. Let (G,ρ) be a permutation representation, and let H be a Hadamard matrix that commutes with all permutation matrices $\rho(g)$. Then the following are elements of a G-equivariant unitary error basis:

$$(U_H)_{ij} = \frac{1}{N} H \circ \mathrm{diag}(H,j)^\dagger \circ H^\dagger \circ \mathrm{diag}(H^T,i). \tag{6}$$

Here $\mathrm{diag}(M,i)$ is the diagonal matrix whose diagonal is the ith row of M.

Proof. It is proven in Ref. [34, Corollary 35] that this is a UEB; showing G equivariance is a simple exercise in matrix algebra. ∎

We will use this construction to prove Theorem IV.5. First, we need the following lemma.

Lemma IV.4. Let M be a circulant matrix of dimension $\geqslant 3$ whose first column vector $(a,b,\ldots,b)$ has first entry a and all other entries b. Let $a = |a|\alpha, b = |b|\beta$, where $\alpha,\beta \in U(1)$ and $|a|,|b| \neq 0$. Then M is unitary precisely when the following conditions are satisfied:

$$\frac{n-2}{n} \leqslant |a| \leqslant 1, \tag{7}$$

$$|b|^2 = \frac{1-|a|^2}{n-1}, \tag{8}$$

$$\mathrm{Re}(\alpha^*\beta) = \frac{2-n}{2}\frac{|b|}{|a|}. \tag{9}$$

Proof. For unitarity, it is sufficient that the rows form an orthonormal basis. It is clear from the symmetry of M that it is sufficient for one row vector to be normal and one pair of row vectors to be orthogonal. This gives us two equations in a and b:

$$|b|^2 = \frac{1-|a|^2}{n-1}, \tag{10}$$

$$\mathrm{Re}(a^*b) = \frac{2-n}{2}|b|^2. \tag{11}$$

We will demonstrate that (7) is necessary and sufficient for us to find b satisfying these equations. It is obvious that (10) is satisfiable if and only if $|a| \leqslant 1$. Letting $a = |a|\alpha, b = |b|\beta$, Eq. (11) then reads as follows:

$$\mathrm{Re}(\alpha^*\beta) = \frac{2-n}{2}\frac{|b|}{|a|}.$$

Since $-1 \leqslant \mathrm{Re}(\alpha^*\beta) \leqslant 1$, and α,β can be freely adjusted to give $\mathrm{Re}(\alpha^*\beta)$ any value in that range, we see that the following is necessary and sufficient for (11) to be soluble:

$$\frac{(2-n)^2}{4}\frac{|b|^2}{|a|^2} \leqslant 1.$$

Use of Eq. (10) and a short calculation demonstrates that this is equivalent to the lower bound in the inequality (7). ∎

Theorem IV.5. There exists a G-equivariant unitary error basis for every permutation representation (G,ρ) of dimension less than 5.

Proof. We use the construction in Proposition IV.3. Expressed in the G-permuted orthonormal basis, $\mathrm{Im}(\rho)$ will be some subgroup of the permutation matrices S_n. To use Theorem IV.3, we must find a Hadamard matrix in the centralizer of $\rho(G)$. In the worst case, $\mathrm{Im}(\rho)$ will be all permutation matrices.

For dimension less than 5, there exists a Hadamard matrix which commutes with all permutation matrices. We ignore the degenerate case $n = 1$. For $n = 2$, the following family of Hadamard matrices commutes with S_2, where $|a| = |b| = 1/\sqrt{2}$ and $\mathrm{Re}(a^*b) = 0$:

$$\begin{pmatrix} a & b \\ b & a \end{pmatrix}.$$

For $n \geqslant 3$, the centralizer of S_n is the group of circulant matrices of the type described in Lemma IV.4; the conditions for such a matrix to be unitary were given there. Setting $|a| = |b|$ in (8), it follows that $|a| = 1/\sqrt{n}$. This is compatible with (7) only for $n \leqslant 4$. ∎

2. Showing nonexistence

In this section, we provide a method for proving nonexistence of an equivariant unitary error basis for some representations (G,ρ).

Definition IV.6. A representation $\rho : G \to U(n)$ on some n-dimensional vector space V is *monomial* [35] if it admits an orthonormal basis of $\mathbb{C}^n$ in which all the matrices $\rho(g), g \in G$ are monomial.

G-equivariant unitary error bases for (G,ρ) are G-equivariant orthonormal bases of $\mathrm{End}(V) \simeq \rho \otimes \rho^*$, all of whose elements are unitary maps. Therefore, if (G,ρ) admits an equivariant UEB, then $\rho \otimes \rho^*$ must be monomial. It is also well known [35] that every monomial representation is a direct sum of representations induced from one-dimensional representations of subgroups. We therefore obtain the following proposition.

Proposition IV.7. If (G,ρ) admits an equivariant UEB, then $\rho \otimes \rho^*$ must split as a direct sum of representations induced from one-dimensional representations of subgroups.

This condition is straightforward to check using characters in a computer algebra program such as GAP [36]. As an example, we exhibit a three-dimensional representation for which no equivariant UEBs exist.

Example IV.8. We show that the three-dimensional irreducible representations of the alternating group A_5 admit no equivariant unitary error basis. In Table II are shown the characters of the induced monomial representations of the

TABLE II. Simple monomial representations for A_5.

()	(1,2)(3,4)	(1,2,3)	(1,2,3,4,5)	(1,2,3,5,4)
1	1	1	1	1
5	1	−1	0	0
5	1	2	0	0
6	−2	0	1	1
6	2	0	1	1

alternating group A_5 of dimension less than or equal to 9. We see that $\chi_{V_i}(1,2,3,4,5) = (\pm\sqrt{5}+1)/2$; this means that $\chi_{V_i\otimes V_i^*}(1,2,3,4,5)$ has a multiple of $\sqrt{5}$ as a summand for both of $i = 1,2$. However, all the monomial characters of A_5 of degree less than 9 have integer values. $\chi_{V_i\otimes V_i^*}$ can therefore not be decomposed as a $\mathbb{Z}_+$-linear combination of monomial characters.

ACKNOWLEDGMENTS

We are grateful to Niel de Beaudrap, Simon Benjamin, Subhayan Moulik, Benjamin Musto, David Reutter, Isar Stubbe, Sean Tull, and Linde Wester for useful discussions. We thank two anonymous referees for their detailed and helpful comments regarding the presentation of these results. We used the blochsphere and solides-3d LaTeX packages. The first author acknowledges support from the Engineering and Physical Sciences Research Council.

APPENDIX A: EXISTENCE OF G-INVARIANT MAXIMALLY ENTANGLED STATES

Here we prove the result stated in Remark II.5.

Definition A.1. A state ω of a G representation is *invariant up to a phase* if $g\omega = \theta(g)\omega$ for some homomorphism $\theta : G \to U(1)$.

Lemma A.2. Let A,B be G representations of identical dimension. A maximally entangled pure state $\omega \in A \otimes B$ invariant up to a phase exists iff $A \simeq \theta \otimes B^*$ for some $\theta : G \to U(1)$.

Proof. Suppose the representation A is the dual of B up to a character θ. Then let ω be the unit $\eta : \mathbb{1} \to \theta^* \otimes A \otimes B$ witnessing the duality $\theta^* \otimes A \simeq B^*$. In the other direction, suppose there exists a state stabilized up to a phase. Any maximally entangled state is of the form

$$\sum_i |i\rangle \otimes X\,|i\rangle$$

for some orthonormal basis $\{|i\rangle\}$ and unitary X. Working in that basis, we have the following, for all $g \in G$, and where $\rho_A(g)^T$ is the transpose in the basis $\{|i\rangle\}$:

$$\begin{aligned} g\sum_i |i\rangle \otimes V\,|i\rangle &= \sum_i \rho_A(g)\,|i\rangle \otimes \rho_B(g)V\,|i\rangle \\ &= \sum_i |i\rangle \otimes \rho_B(g)V\rho_A(g)^T\,|i\rangle. \end{aligned}$$

It follows that $\rho_B(g)V\rho_A(g)^T = \theta(g)V$, and therefore that $\rho_B(g) = \theta(g)V\rho_A(g)^*V^\dagger$ for all g, where $\rho_A(g)^*$ is the complex conjugate matrix. The result follows by definition of the dual representation. ∎

APPENDIX B: PROOF OF CLASSIFICATION OF QUBIT UNITARY ERROR BASES

In this appendix, we prove Theorem IV.1. We begin by fixing some notation for rotations. Euler showed [37] that every rotation in SO(3) can be represented uniquely as a rotation through an angle $0 \leqslant \theta \leqslant \pi$ around a given normalized vector $\hat{n} \in \mathbb{R}^3$. We write a rotation through an angle θ around an axis $\hat{n}$ as $r(\theta,\hat{n})$.[6] Given two rotations $r(\theta_1,\hat{n}_1)$ and $r(\theta_2,\hat{n}_2)$, we write the angle and axis of the composite as θ_{12} and $\hat{n}_{12}$. For concision, we will occasionally write rotations simply as $r \in \mathrm{SO}(3)$, omitting to mention the axis and angle of rotation.

It is well known that unitary operations on a qubit correspond to rotations of the Bloch sphere together with a global phase [38, Exercise 4.8]. It is easy to check that two unitaries U_1,U_2 are orthogonal iff their corresponding Bloch sphere rotations $q(U_1),q(U_2)$ are orthogonal in the following sense.

Definition B.1. Two rotations $r_1,r_2 \in \mathrm{SO}(3)$ are *orthogonal* if the composite $r_1^{-1}r_2$ is a rotation through the angle π.

The image of a UEB under the quotient q will be a set of orthogonal rotations preserved under conjugation by the orthogonal rotations $q(\rho(g))$ for $g \in G$; this inspires the following definition.

Definition B.2. An *orthogonal error basis* (OEB) is a family $\mathcal{O} \subset \mathrm{SO}(n)$ of n^2 orthogonal rotations. For a finite group G and a homomorphism $\rho : G \to \mathrm{SO}(n)$, an *equivariant orthogonal error basis* for (G,ρ) is an OEB $\mathcal{O} \subset \mathrm{SO}(n)$ preserved under conjugation by $\rho(g)$ for all $g \in G$.

In the other direction, given an equivariant OEB for $(G,q \circ \rho)$, one may obtain all corresponding equivariant UEBs for (G,ρ) by picking phases for each rotation. A classification of equivariant UEBs for subgroups $G \subset \mathrm{U}(2)$ is therefore equivalent to a classification of equivariant OEBs for subgroups $q(G) \subset \mathrm{SO}(3)$. Note also that the action of $\rho(g)$ on the index set of a UEB is identical to the action of $q(\rho(g))$ on the index set of the corresponding OEB.

Theorem B.3 ([39, Theorem 19.2]). The finite subgroups of SO(3) are as follows:

(1) cyclic groups $\mathbb{Z}_n$ for $n \geqslant 1$, generated by a rotation through $2\pi/n$ around a given axis;

(2) dihedral groups D_n for $n \geqslant 1$, generated by a rotation through $2\pi/n$ around a given axis and a π rotation around a perpendicular axis;

(3) the group of orientation-preserving symmetries of a regular tetrahedron, isomorphic to A_4;

(4) the group of orientation-preserving symmetries of a regular octahedron (or a cube), isomorphic to S_4;

(5) the group of orientation-preserving symmetries of a regular icosahedron, isomorphic to A_5.

In order to find sets of points preserved under the conjugation action of these subgroups, we recall a useful way to think about conjugation in SO(3). The group SO(3) may be viewed as a closed ball $\mathrm{B}(3) \subset \mathbb{R}^3$ of radius π, which we call the SO(3) ball, under the identification

$$r(\theta,\hat{n}) \mapsto \theta\hat{n}. \tag{B1}$$

Antipodal points on the boundary are identified, since rotation through an angle π around $\hat{n}$ is the same as rotation through an angle π around $-\hat{n}$. Given two rotations $r_1 = r(\theta,\hat{n})$ and r_2, we have the identity

$$r_2r_1r_2^{-1} = r_2r(\theta,\hat{n})r_2^{-1} = r(\theta,r_2(\hat{n})).$$

[6] Note that this notation is slightly redundant because rotations through an angle π around antipodal $\hat{n}$ are identical, as are all rotations through an angle 0.

It follows that, under the identification (B1), conjugation by a rotation in SO(3) corresponds to rotation of the SO(3) ball. Equivariant OEBs for a subgroup are therefore sets of orthogonal points in the SO(3) ball permuted by rotations in that subgroup.

For concision, in what follows we will occasionally conflate points in B(3) and rotations in SO(3). For instance, we say "a point on the z axis" to signify the element of SO(3) corresponding to a point on the z axis, that is, a rotation around the z axis through some angle. We will also write $\sin(x)$, $\cos(x)$, and $\tan(x)$ as $\sin(x)$, $\cos(x)$, and $\tan(x)$ respectively.

We now recall some useful facts about orthogonality in SO(3).

Lemma B.4. Each rotation in SO(3) around $\hat{n}$ is orthogonal to exactly one other rotation around $\pm\hat{n}$.

Proof. The composite $r(\theta_1,\hat{n})^{-1}r(\theta_2,\hat{n})$ is the rotation $r(\theta_2-\theta_1,\hat{n})$. For a given $\theta_1 \in [0,\pi]$, there is only one $\theta_2 \in (-\pi,\pi]$ such that $\theta_1-\theta_2$ is an odd multiple of π. ■

Lemma B.5. The rotation $r(\theta_2,\hat{n}_2)$ is orthogonal to the rotation $r(\pi,\hat{n}_1)$ iff either $\hat{n}_2$ is orthogonal to $\hat{n}_1$ or $\theta_2 = 0$.

Proof. We have the following standard formula for the rotation angle θ_{12} of the composite $r_2^{-1}\circ r_1$, where r_i is a rotation around the axis $\hat{n}_i$ through an angle $\theta_i \in [0,\pi]$ [38, Exercise 4.15]:

$$\cos(\theta_{12}/2) = \cos(\theta_1/2)\cos(\theta_2/2) + \sin(\theta_1/2)\sin(\theta_2/2)\hat{n}_1\cdot\hat{n}_2. \quad \text{(B2)}$$

Orthogonality of r_2 and r_1 is precisely the condition that the left-hand side (LHS) is zero. Since the first term on the right-hand side (RHS) equals zero when $\theta_1 = \pi$, the second term must also. This implies that either $\hat{n}_1\cdot\hat{n}_2 = 0$, in which case the axes of rotation are orthogonal, or $\sin(\theta_2/2) = 0$, in which case the other rotation is simply the identity. ■

Lemma B.6. Two rotations can be orthogonal only if the angle between the axes of rotation is obtuse. If the angle between the axes is $\pi/2$ then for orthogonality one rotation must be through the angle π.

Proof. Considering (B2), we note that both $\cos(\theta_1/2)\cos(\theta_2/2)$ and $\sin(\theta_1/2)\sin(\theta_2/2)$ will be positive for $\theta_1,\theta_2 \in [0,\pi]$. The sum can only be zero, then, if $\hat{n}_1\cdot\hat{n}_2 \leqslant 0$, i.e., if the angle between the axes is obtuse. If the angle is $\pi/2$ then we need $\cos(\theta_1/2)\cos(\theta_2/2) = 0$, which implies that one of the rotations is through an angle π. ■

We now begin our classification.

a. Cyclic subgroups of SO(3)

Any set of orthogonal points will be equivariant for $\mathbb{Z}_1$. We proceed directly to the nontrivial cases. Let the z axis be the axis of rotation of the generator of $\mathbb{Z}_n$ which rotates the SO(3) ball through an angle $2\pi/n$. Recalling that antipodal points on the ball's surface are identified, we immediately obtain the following characterization of the orbits under this action.

Lemma B.7. The orbit sizes under the conjugation action of $\mathbb{Z}_n$ on SO(3) are as follows:

(1) 1, for a point on the axis of rotation;

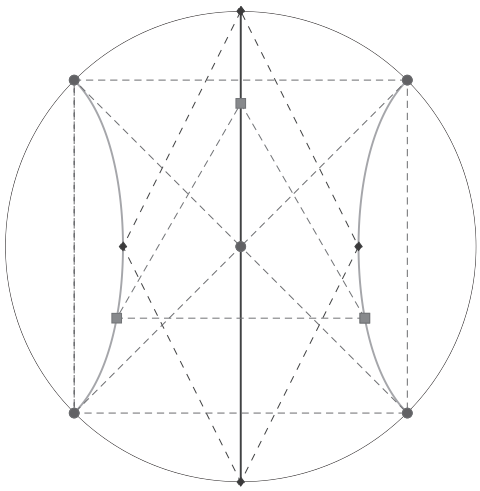
(2) n, for a point in the interior of the ball and not on the axis of rotation, on the boundary of the ball and not on the xy plane or the axis of rotation, or on the intersection of the boundary of the ball and the xy plane when n is odd;

(3) $n/2$, for a point on on the intersection of the boundary of the ball and the xy plane when n is even.

Proposition B.8. The $\mathbb{Z}_2$-equivariant orthogonal error bases are as follows:

(1) for orbit type (1,1,1,1), a two-parameter family of solutions, where two points are rotations around the z axis and the other two are π rotations around orthogonal axes in the xy plane;

(2) for orbit type (2,1,1), a two-parameter family of solutions, where one point is a rotation around the z axis, another point is a π rotation around an x axis perpendicular to the z axis, and the other two points are rotations around axes in the yz plane (see Fig. 3), where the y axis is perpendicular to both the x and z axes;



OEB	Elements
1	π around z, $\pm\pi/2$ around y
2	Identity, π around $y \pm z$
3	$2\arccos(\sqrt{1/3})$ around z, $\pm 3y - z$

FIG. 3. $\mathbb{Z}_2$-equivariant OEBs with orbit type (2,1,1). The diagram shows the intersection of the yz plane with the SO(3) ball. One 1-orbit of the OEB is a π rotation around the x axis, and the remaining 2-orbit and 1-orbit are rotations around axes in the yz plane shown in the diagram. Each 2-orbit is a pair of points with identical z value on the two curved gray lines. The corresponding 1-orbit is a point on the z axis. Three possible choices of points are given in the table and marked in the figure, joined by dashed lines.

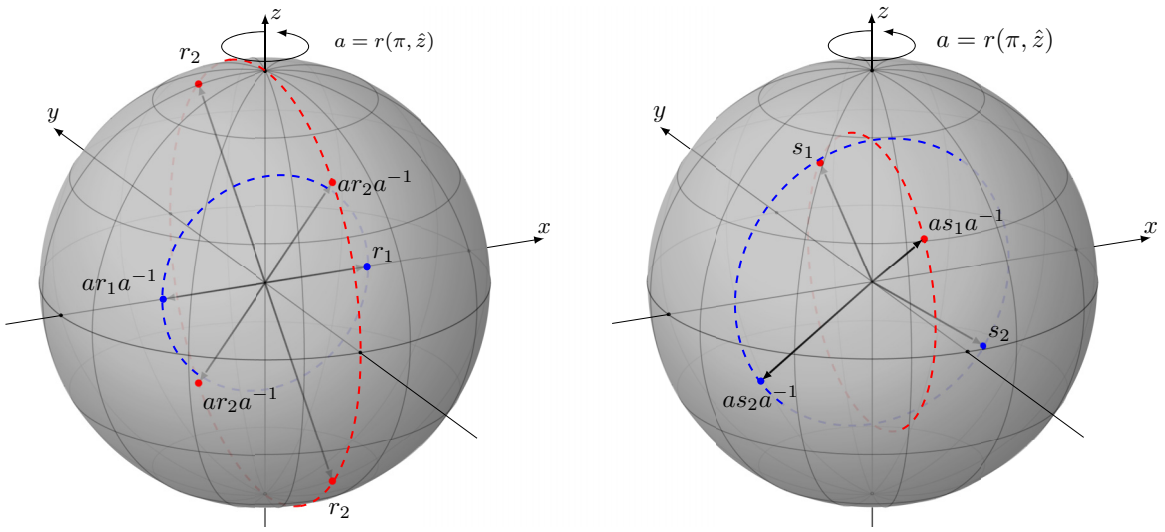


FIG. 4. Two equivariant OEBs for $\mathbb{Z}_2$ with orbit type (2,2), pictured in the SO(3) ball. Under the $\mathbb{Z}_2$ action, the equivariant OEB on the left is generated by $r_1 = r(\pi/2,\hat{x})$ and $r_2 = r(\pi, \frac{1}{\sqrt{2}}(\hat{y} + \hat{z}))$ (note the identification of antipodal points), while the equivariant OEB on the right is generated by $s_1 = r(2\pi/3, \frac{1}{\sqrt{3}}(\sqrt{2}\hat{y} + \hat{z}))$ and $s_2 = r(2\pi/3, \frac{1}{\sqrt{3}}(\sqrt{2}\hat{x} - \hat{z}))$.

(3) for orbit type (2,2), a two-parameter family of solutions, where, for an axis x orthogonal to z and an axis y orthogonal to both, two points lie in the xz plane and below the xy plane, and another two points lie in the yz plane and above the xy plane (see Fig. 4).

Proof. Orbit type (1,1,1,1). By Lemma B.4, there can be at most two rotations on the z axis. The other two, in order to have orbit size 1, must both be π rotations around different axes in the xy plane, which must be orthogonal to each other by Lemma B.5. This set of solutions therefore has two independent parameters, namely the angle of one rotation around the z axis and the orientation of the perpendicular axes in the xy plane.

Orbit type (2,1,1). First, suppose both the 1-orbits lie off the z axis. Then they must be orthogonal π rotations in the xy plane. But then the other two rotations would have to be orthogonal and we would end up in the case (1,1,1,1).

Let us now suppose that exactly one of the 1-orbits lies on the z axis. The other must be an orthogonal π rotation; let this be around the x axis. Then the 2-orbit must lie in the yz plane by Lemma B.5. We are therefore looking for three orthogonal points in the yz plane, one on the z axis and the other two symmetric under a reflection in the z axis. Let r be the rotation angle of the elements in the 2-orbit and θ be the angle between them. Here we take $0 < \theta < 2\pi$, where $\theta = 0$ would correspond to both points being on the positive z axis. By (B2) we have the following equation for orthogonality of the elements of the 2-orbit:

$$r = 2\cos^{-1}\left(\sqrt{\frac{\cos(\theta)}{\cos(\theta) - 1}}\right). \tag{B3}$$

This has a unique solution $r \in [\pi/2,\pi]$ for $\theta \in [\pi/2,3\pi/2]$, and none otherwise. Using (B2), it can be shown similarly that, for given θ, there is a unique value of the z coordinate of the 1-orbit such that all three points are orthogonal (see Fig. 3). We therefore have a two-parameter family of solutions, where one parameter corresponds to a choice of z-coordinate z_1 of the 1-orbit on the z axis, and the other parameter comes from a choice of orientation of the x axis.

Suppose now that both 1-orbits lie on the z axis; we will demonstrate that we cannot then obtain solutions of this orbit type. First, if the elements of the 2-orbit are π rotations not in the xy plane, then they will not be orthogonal to the 1-orbits on the z axis. On the other hand, if the elements of the 2-orbit are rotations through an angle less than π and not in the xy plane, then, given that by Lemma B.4 the z rotations will be on opposite sides of the origin, both elements of the 2-orbit will make an acute angle with one of the z rotations, violating Lemma B.6. The 2-orbit must therefore lie in the xy plane. The rotations of the 2-orbit must be through an angle less than π, or they would form two 1-orbits. But, by Lemma B.6, in order to be orthogonal both z rotations must then be through an angle π, which would identify them.

Orbit type (2,2). Each 2-orbit will lie in a plane through the z axis. Again, let r be the rotation angle of the elements in the 2-orbit and θ be the angle between them; the relationship between r and θ was already given in (B3).

We must find two 2-orbits where all four elements are pairwise orthogonal. Without loss of generality, let the first orbit O_1 lie in the xz plane and let $\theta_1 \in [\pi/2,\pi]$. Certainly, the second orbit O_2 must have $\theta_2 \in [\pi,3\pi/2]$, as otherwise the central angle between some pair of elements will be acute. We now show that the orbit O_2 must also lie in the yz plane. In other words, the two 2-orbits must lie in orthogonal planes containing the z axis, and be on opposite sides of the xy plane.

Let $r_1,r_2 \in [0,\pi]$ be the rotation angles of O_1 and O_2 respectively. Take one element from each orbit and consider their composition (B2). With r_1,r_2 fixed, the only thing that can vary on the right-hand side of this equation is the angle between the axes of rotation of these elements. This angle will

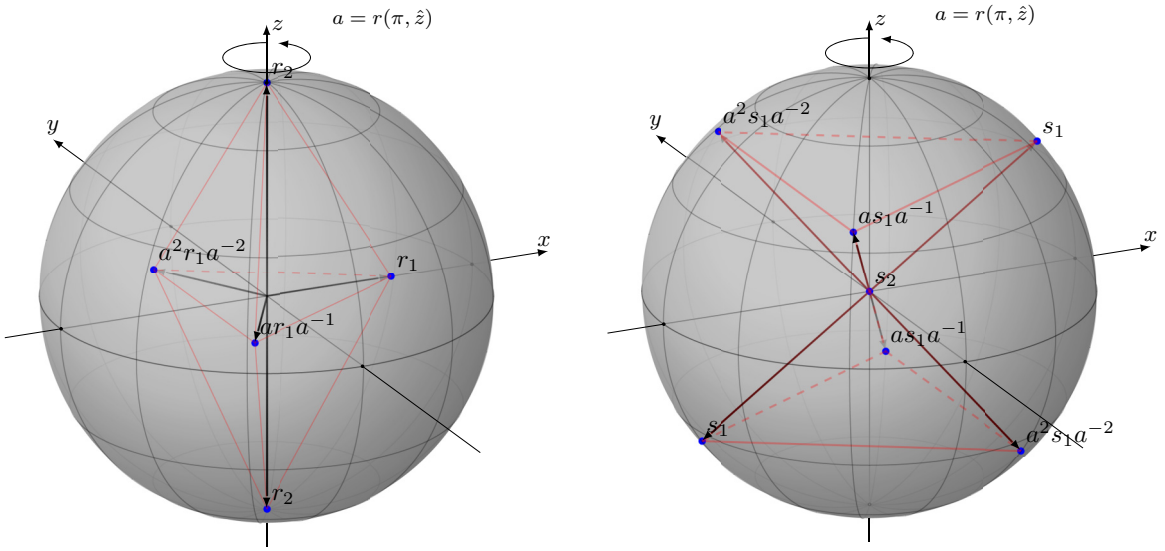


FIG. 5. Two equivariant OEBs for $\mathbb{Z}_3$ with orbit type (3,1). Under the $\mathbb{Z}_3$ action, the equivariant OEB on the left is generated by $r_1 = r(2\sin^{-1}(\sqrt{\frac{2}{3}}),\hat{x})$ and $r_2 = r(\pi,\hat{z})$, and the equivariant OEB on the right is generated by $s_1 = r(\pi, \frac{1}{\sqrt{3}}(\sqrt{2}\hat{x} + \hat{z}))$ and $s_2 = r(0,\hat{z})$. Note the identification of antipodal points in both cases; this is why the points are vertices of two tetrahedra rather than just one.

lie between 0 and π, and $\cos(x)$ is single-valued in that range; therefore, for both elements of the second orbit to be orthogonal to the given element of the first, their axes of rotation must both have an equal central angle with that element. This means that the xz plane containing O_1 must be orthogonal to the plane through the z axis containing O_2, which must therefore be the yz plane.

With the planes fixed, we now find which angles $\theta_1 \in [\pi/2,\pi]$ and $\theta_2 \in [\pi,3\pi/2]$ defining the two orbits are compatible. By the above discussion, for orthogonality of all elements it is sufficient for a single pair of elements from different orbits to be orthogonal. Unit vectors $\hat{n}_1,\hat{n}_2$ defining the axes of rotation of a pair of elements in O_1, O_2 respectively may be expressed in Cartesian coordinates as $\hat{n}_1 = (\sin(\theta_1/2),0,\cos(\theta_1/2))$ and $\hat{n}_2 = (0,\sin(\theta_2/2),\cos(\theta_2/2))$. The orthogonality condition (B2) then becomes

$$-\cos(r_1/2)\cos(r_2/2) = \sin(r_1/2)\sin(r_2/2)\cos(\theta_1/2)\cos(\theta_2/2). \tag{B4}$$

Replacing θ_1,θ_2 with r_1,r_2 using (B3), squaring both sides, and performing some trigonometric manipulations, we derive

$$r_1 = 2\cos^{-1}\left(\sqrt{\frac{1}{2} - \cos^2\left(\frac{r_2}{2}\right)}\right).$$

This uniquely determines $r_1 \in [\pi/2,\pi]$ for any $r_2 \in [\pi/2,\pi]$. The solutions of orbit type (2,2) are therefore parametrized by two angle variables; the first is the orientation of the x axis and the second is the angle r_2 of one of the rotations in the 2-orbit O_2 lying below the xy plane. Two of these solutions are shown in Fig. 4. ■

Proposition B.9. The $\mathbb{Z}_3$-equivariant orthogonal error bases are as follows:

(1) for orbit type (1,1,1,1), no solutions;

(2) for orbit type (3,1), a two-parameter family of solutions, forming the vertices of a tetrahedron with one vertex on the z axis and the other three forming an equilateral triangle in a plane perpendicular to the z axis (see Fig. 5).

Proof. Orbit type (1,1,1,1). All the points would need to be on the z axis, which is impossible by Lemma B.4.

Orbit type (3,1). By the classification of orbits (Lemma B.7), these OEBs consist of a 1-orbit on the z axis and a 3-orbit forming the vertices of an equilateral triangle in a plane perpendicular to the z axis. Let one of the elements in the 3-orbit lie in the xz plane, so $(r,\psi,0)$ are its spherical coordinates. From (B2), we obtain the following condition for orthogonality of the elements of the 3-orbit:

$$r = 2\sin^{-1}\left(\frac{\sqrt{2}}{\sqrt{3}\sin(\psi)}\right).$$

Where soluble, this equation completely determines r for given ψ. It admits solutions for $\psi \in [\sin^{-1}(\sqrt{\frac{2}{3}}),\pi - \sin^{-1}(\sqrt{\frac{2}{3}})]$. By (B2), we also obtain an equation in ψ for the height z of the point on the z axis, which is single valued in the range $\psi \in [\sin^{-1}(\sqrt{\frac{2}{3}}),\pi - \sin^{-1}(\sqrt{\frac{2}{3}})]$:

$$z = 2\tan^{-1}\left(\sqrt{\frac{3}{2}}\cos(r(\psi)/2)\tan(\psi)\right).$$

Under this equation, z can take all values in $[-\pi,\pi]$; the 3-orbit lies on the other side of the xy plane. These OEBs therefore form a two-parameter family, where one parameter is the angle ψ, and the other is the choice of x axis. Two solutions are shown in Fig. 5. ■

Proposition B.10. The $\mathbb{Z}_4$-equivariant orthogonal error bases are as follows:

(1) for orbit type (1,1,1,1), no solutions;

(2) for orbit type (2,1,1), a two-parameter family of solutions identical to the (1,1,1,1) solutions for $\mathbb{Z}_2$ (Proposition B.8);
(3) for orbit type (2,2), no solutions;
(4) for orbit type (4), no solutions.

Proof. Orbit type (1,1,1,1). All the points would need to be on the z axis, which is impossible by Lemma B.4.

Orbit type (2,1,1). The 2-orbit must consist of orthogonal π rotations around axes in the xy plane. One parameter therefore corresponds to the rotation angle of one of the rotations on the z axis, and the other to the orientation of the orthogonal axes in the the xy plane.

Orbit type (2,2). These must be four different π rotations around axes in the xy plane. But then they cannot be orthogonal.

Orbit type (4). The angle between rotation vectors in a 4-orbit will be acute if they are not in the xy plane, so they cannot be orthogonal. If they are in the xy plane, then as the angle between adjacent vectors is $\pi/2$, at least one pair of opposite vectors must be π rotations by Lemma B.6; but then these will be identified and this will not be a 4-orbit. ■

Proposition B.11. There are no $\mathbb{Z}_n$-equivariant orthogonal error bases for $n \geqslant 5$.

Proof. We handle the odd and even cases separately.

$n \geqslant 5$ *and n odd*. The only orbit sizes are 1 and n. Since we only have four elements in the UEB, all four points must be of orbit size 1; they must therefore all be on the $\hat{z}$ axis. But this is impossible by Lemma B.4.

$n \geqslant 5$ *and n even*. For $n = 6$, the orbit sizes are 1, 3, and 6. Since for the reason given above we cannot have four 1-orbits, we must have one 1-orbit and one 3-orbit. However, the axes of the π rotations will not be orthogonal and so the rotations are not orthogonal by Lemma B.5. For $n = 8$, the orbit sizes are 1,4, and 8, so we are forced to have a 4-orbit by Lemma B.4. But these π rotations will again not be around orthogonal vectors and are therefore not orthogonal by Lemma B.5. For $n > 8$, the orbit sizes for elements off the $\hat{z}$ axis are all greater than 4.

b. Dihedral subgroups of SO(3)

Let the z axis be the axis of cyclic rotation, and let the f axis be the perpendicular axis of π rotation (the "flip axis").

Proposition B.12. The D_2-equivariant orthogonal error bases are as follows:
(1) for orbit type (1,1,1,1), one solution;
(2) for orbit type (2,1,1), six solutions;
(3) for orbit type (2,2), three solutions;
(4) for orbit type (4), two solutions.

Proof. Any solution for D_2 must also be a solution for its $\mathbb{Z}_2$ subgroup, and we proceed by case analysis of $\mathbb{Z}_2$-orbit types, making use of Proposition B.8.

$\mathbb{Z}_2$-orbit type (1,1,1,1). Recall that $\mathbb{Z}_2$-equivariant OEBs of this type are made up of two π rotations around orthogonal axes in the xy plane and two rotations around the z axis. If we fix the flip axis f, in order that the rotations in the xy plane are preserved there are two choices for the axes: either f and g, or $f + g$ and $f - g$. In order that the z rotations are preserved, there are two choices for the rotation angles: either 0 and π, or $-\pi/2$ and $\pi/2$. The orbit types are (1,1,1,1), (2,1,1), (2,1,1), and (2,2).

$\mathbb{Z}_2$-orbit type (2,1,1). Recall that $\mathbb{Z}_2$-equivariant OEBs of this type are made up of a π rotation around some x axis, a rotation around the z axis, and two other rotations around axes in the yz plane (see Fig. 3). Fix the flip axis f. The z rotation will be preserved under the flip only if it is through an angle π or 0. This fixes the rotation angle r of the elements in the 2-orbit as $\pi/2$ or π respectively. For the x rotation to be preserved under the flip, we need either that $x = f$ or $y = f$. In both of these cases, the solutions with $r = \pi/2$ and $r = \pi$ are preserved. We therefore obtain four equivariant OEBs with orbit type (2,1,1).

$\mathbb{Z}_2$-orbit type (2,2). Consider the 2-parameter family of solutions of orbit type (2,2). The 2-orbits O_1, O_2 lie on opposite sides of the xy plane, in the xz and yz planes respectively. D_2 is Abelian, so the $\mathbb{Z}_2$-orbit pairing will be preserved after the flip. There are therefore two possibilities if the elements are to be preserved under the flip; the flip can either swap the xz and yz planes or preserve them.

If the planes are preserved, then the flip axis must be the x or y axis, and the 2-orbits must be symmetric under reflection in the xy plane. Since one orbit is fixed by the other, this gives two solutions of orbit type (2,2), corresponding to a choice of $r_1 = \pi/2$ or $r_1 = \pi$ in O_1, where r_i is the rotation angle of the elements of O_i (see Fig. 3).

If the planes are permuted then the flip axis must be $v_1 \pm v_2$, and $r_1 = r_2$. Setting $r_1 = r_2$ in (B4) and substituting in (B3), we obtain $\cos(\theta) = -\frac{1}{3}$, where $\theta \in [\pi/2,\pi]$ is the central angle between the elements of each orbit. This has a unique solution in the relevant domain of orbit type (4). There are two of these for a given choice of f axis, since we can choose which orbit lies above the xy plane. ■

Proposition B.13. There are six isolated D_3-equivariant quotient orthogonal error bases all of orbit type (3,1).

Proof. Any solution for D_3 must also be a solution for its $\mathbb{Z}_3$ subgroup. In Proposition B.9 we saw that solutions were the vertices of a two-parameter family of tetrahedra with one vertex on the z axis and the others forming the vertices of an equilateral triangle on the other side of the xy plane. The vertex on the z-axis point must be preserved under reflection in the xy plane, so it must be through an angle 0 or π; the two possibilities were shown in Figure 5. For $z = 0$, the elements of the 3-orbit will be preserved if the fz plane is orthogonal to the triangle's medians, giving three solutions. For $z = \pi$, the f axis must go through any of the three vertices of the triangle, giving three solutions. ■

Proposition B.14. The D_4-equivariant orthogonal error bases are as follows:
(1) for orbit type (2,1,1), two isolated solutions;
(2) for orbit type (2,2), two isolated solutions.

Proof. Any solution for D_4 must also be a solution for its $\mathbb{Z}_4$ subgroup. In Proposition B.10, we saw that these form a single two-parameter family; they can only be preserved if $f = x$ or $f = x + y$, and the points on the z axis are either $\{0,\pi\}$, which yields orbit type (2,1,1), or $\{-\pi/2,\pi/2\}$, which yields orbit type (2,2). ■

Proposition B.15. There are no D_n-equivariant orthogonal error bases for $n \geqslant 5$.

Proof. If there is no equivariant OEB for the cyclic subgroup, there can be none for the full dihedral group. The result therefore follows from Proposition B.11. ■

c. Other subgroups of SO (3)

Proposition B.16. The tetrahedral subgroups have two equivariant orthogonal error bases, both of orbit type (4).

Proof. Any solution for the tetrahedral group must also be a solution for its $\mathbb{Z}_3$ subgroup. These form a two-parameter family of tetrahedra. Since the tetrahedral group preserves only a regular tetrahedron and its dual, there will be exactly two solutions corresponding to the vertices of those tetrahedra. ■

Proposition B.17. The octahedral subgroups have one equivariant orthogonal error basis of orbit type (1,3).

Proof. Any solution for the octahedral group must also be a solution for its D_4 subgroup. Only one of these equivariant for the full octahedral group, with three points at the face centers of a cube of center-to-face length π, and the final point at the origin. ■

Proposition B.18. The icosahedral subgroups have no equivariant orthogonal error bases.

Proof. There is no equivariant OEB for the D_5 subgroup, so there will be none for the full icosahedral group. ■

[1] S. D. Bartlett, T. Rudolph, and R. W. Spekkens, Rev. Mod. Phys. **79**, 555 (2007).

[2] A. Kitaev, D. Mayers, and J. Preskill, Phys. Rev. A **69**, 052326 (2004).

[3] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).

[4] F. Verstraete and J. I. Cirac, Phys. Rev. Lett. **91**, 010404 (2003).

[5] G. Gour and R. W. Spekkens, New J. Phys. **10**, 033023 (2008).

[6] S. J. van Enk, J. Mod. Opt. **48**, 2049 (2001).

[7] J. Wabnig, D. Bitauld, H. W. Li, A. Laing, J. L. O'Brien, and A. O. Niskanen, New J. Phys. **15**, 073001 (2013).

[8] J. L. Duligall, M. S. Godfrey, K. A. Harrison, W. J. Munro, and J. G. Rarity, New J. Phys. **8**, 249 (2006).

[9] J. L. Duligall, M. S. Godfrey, A. M. Lynch, W. J. Munro, K. J. Harrison, and J. G. Rarity, in *CLEO Europe and IQEC 2007 Conference Digest* (Optical Society of America, Munich, Germany, 2007).

[10] J.-G. Ren, P. Xu, H.-L. Yong, L. Zhang, S.-K. Liao, J. Yin, W.-Y. Liu, W.-Q. Cai, M. Yang, L. Li *et al.*, Nature (London) **549**, 70 (2017).

[11] J. Yin, Y. Cao, Y.-H. Li, S.-K. Liao, L. Zhang, J.-G. Ren, W.-Q. Cai, W.-Y. Liu, B. Li, H. Dai *et al.*, Science **356**, 1140 (2017).

[12] L. Bacsardi, IEEE Commun. Mag. **51**, 50 (2013).

[13] T. Islam, L. Magnin, B. Sorg, and S. Wehner, New J. Phys. **16**, 063040 (2014).

[14] T. Islam and S. Wehner, New J. Phys. **18**, 033018 (2016).

[15] M. Skotiniotis and G. Gour, New J. Phys. **14**, 073022 (2012).

[16] S. D. Bartlett, T. Rudolph, and R. W. Spekkens, Phys. Rev. A **70**, 032307 (2004).

[17] L. M. Ioannou and M. Mosca, Theor. Comput. Sci. **560**, 33 (2014).

[18] V. D'Ambrosio, E. Nagali, S. P. Walborn, L. Aolita, S. Slussarenko, L. Marrucci, and F. Sciarrino, Nat. Commun. **3**, 961 (2012).

[19] P. Zhang, K. Aungskunsiri, E. Martín-López, J. Wabnig, M. Lobino, R. W. Nock, J. Munns *et al.*, Phys. Rev. Lett. **112**, 130501 (2014).

[20] C. Wang, S.-H. Sun, X.-C. Ma, G.-Z. Tang, and L.-M. Liang, Phys. Rev. A **92**, 042319 (2015).

[21] W.-Y. Liang, S. Wang, H.-W. Li, Z.-Q. Yin, W. Chen, Y. Yao, J.-Z. Huang, G.-C. Guo, and Z.-F. Han, Sci. Rep. **4**, 3617 (2014).

[22] C. E. R. Souza, C. V. S. Borges, A. Z. Khoury, J. A. O. Huguenin, L. Aolita, and S. P. Walborn, Phys. Rev. A **77**, 032345 (2008).

[23] A. Laing, V. Scarani, J. G. Rarity, and J. L. O'Brien, Phys. Rev. A **82**, 012304 (2010).

[24] G. Vallone, V. D'Ambrosio, A. Sponselli, S. Slussarenko, L. Marrucci, F. Sciarrino, and P. Villoresi, Phys. Rev. Lett. **113**, 060503 (2014).

[25] G. Chiribella, V. Giovannetti, L. Maccone, and P. Perinotti, Phys. Rev. A **86**, 010304 (2012).

[26] U. Marzolino and A. Buchleitner, Phys. Rev. A **91**, 032316 (2015).

[27] U. Marzolino and A. Buchleitner, Proc. R. Soc. London, Ser. A **472** (2016).

[28] D. Verdon and J. Vicary, arXiv:1802.09040 (unpublished).

[29] A. Peres and P. F. Scudo, in *Quantum Theory: Reconsideration of Foundations*, edited by A. Khrennikov (Växjö Univesity Press, Växjö (smaland), Sweden, 2002).

[30] M. Skotiniotis, W. Dür, and B. Kraus, Quantum Inf. Comput. **13**, 0290 (2013).

[31] R. F. Werner, J. Phys. A: Math. Gen. **34**, 7081 (2001).

[32] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, Phys. Rev. Lett. **70**, 1895 (1993).

[33] D. Verdon and J. Vicary, Electronic Proceed. Theor. Comp. Sci. **236**, 202 (2017).

[34] B. Musto and J. Vicary, Quantum Inf. Comput. **16**, 1318 (2016).

[35] C. W. Curtis and I. Reiner, *Representation Theory of Finite Groups and Associative Algebras*, AMS Chelsea Publishing Series (Interscience, Providence, Rhode Island, 1966).

[36] GAP: Groups, Algorithms, and Programming, version 4.8.6 (GAP Group, 2016), https://www.gap-system.org/.

[37] L. Euler, Novi Commentarii academiae scientiarum Petropolitanae **20**, 189 (1776).

[38] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*, 10th ed. (Cambridge University Press, New York, 2011).

[39] M. A. Armstrong, *Groups and Symmetry*, Undergraduate Texts in Mathematics (Springer, New York, 1997).